Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Deloitte & Touche LLP*
Name of Submitter/POC:	*Badrinath Nemani*
Email Address of Submitter/POC:	[redacted]

A	(Base, 63A, 63B, 63C)	Section	Page #	Line #	(Include rationale for comment)	Suggested Change
	63-Base	3.4.1.	42	1581	"Threat Resistance" should consider likelihood, a key element of risk. However, the focus of this section appears to be solely on impact—for example, lines 937, 940, and 943 state, "What negative impacts would reasonably be expected if..." According to NIST SP 800-39, "Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (i.e., magnitude of harm) to organizations, assets, and individuals."	Add consideration of the likelihood into the assessment. The likelihood of an impact should have a significant bearing on the risk tailoring process. For example, an invitation only system may have a much lower likelihood of IAL-related incidents than an open-to-the-public system. The invitation process could also be used as a compensating control in the tailoring process.
	63-Base	3.5.1	45	1693	For clarity sake, this text would benefit from clarification/revision: "as well as validation, verification, and fraud management systems as appropriate". There is no definition of the terms "validation systems" or "verification systems" in the document (though validation and verification are steps in the ID Proofing process). The language may confuse readers into thinking separate systems are needed for each step in the process to support digital identity.	Clarify: " as well as validation, verification, and fraud management systems as appropriate"
	63-Base	Table 4	46	1715	(A) For clarity, we suggest being consistent with regard to "process" and "process step". Note Column1 "Failure Rates (Per Proofing Process Step)" versus Column 2 in the two rows above "failing a process". (B) Also, the last row has a typo. The "(" should be after "Times" to read: "Completion Times (Per Proofing Type)"	(A) Recommend clarifying what is meant by "process steps" and being more consistency. For example, why is abandonment rate "Per Proofing Type " and Failure Rates "Per Proofing Process Step". Fix the typo
	63-Base	3	22	925	To include more specifics for Identity Ecosystem Optimization on what context from the broader identity ecosystem may be relevant for a given transaction, or user identity for the Digital Identity Risk Management (DIRM) process.	Organizations should therefore be required to consider (1) whether a user currently has, or is likely to require, access to a different online services requiring different solutions, whether the user currently has access to a similar online services through an organization they can federate with, and whether the organization has identity solutions available internally that could be used for the transaction at issue. Organizations should also maintain inventories of users accounts, services and identities (can be deidentified to protect privacy), with metrics to evaluate optimization of the ecosystem.
	63A	2.4	10	646	Figure 1 says: "*1 Resolution* - Core attributes and evidence collected." So, according to Figure 1, evidence is collected as part of Resolution. However, Section 2.3, *Identity Resolution* , makes no mention of evidence collection. Instead, the first line in Section 2.4, *Identity Validation and Identity Evidence Collection* , says, "the goal of identity validation is to collect the most appropriate identity evidence from the applicant." The narrative, including section structure, should be consistent with the figure.	Align the narrative and the figure. The Figure seems more accurate since you shouldn't perform resolution based on no evidence at all. Move 2.4.1 and its subsections under 2.3. Also, change the begining of of 2.4 to: "The goal of identity validation is to ~~collect the most appropriate identity evidence from the applicant and~~ determine that ~~it~~ the evidence collected is genuine (not altered or forged), accurate (the pertinent data is correct, current, and related to the applicant), and valid."
	63A	2.4.1.2	11	699	"5. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates." Many people will avoid submitting images of their Photo ID over the internet in order to obtain government services due to concerns about protecting their privacy. Requiring people to provide an image of a Photo ID online in order to obtain service will result in an increase in the illicit collection and sharing of these ID document images. Like a social security number, the documents are not secret. They are shown frequently in physical interactions (their intended use) to show proof of age, etc. Also like a social security number, people do not want their ID documents widely shared.	Rethink requiring Photo ID for IAL2 in favor of a more balanced, user-centric, and flexible approaches that are more equitable. Consider that there are other, user-centric options that may be more pallatable for those people that don't require a Photo ID, such as W3C verifiable credentials, which leverages blockchain technology to securely link authentication and transactional information. Also, consider the Real ID compliant programs states employ which include a flexibile mixture of evidence in terms of quantity and strength rather than one Photo ID and one Non-Photo ID (the basic requirements for IAL2), e.g., https://dmv.ny.gov/forms/id82.pdf.
	63A	3.2	35	1492	Regarding: " 4. CSPs SHOULD avoid collecting, validating, and verifying previously processed evidence, though they MAY do so *based on the age of the account*, [...]" The language potentially undermines one of the strongest pieces of identity evidence -- that of a historical and ongoing relationship. The age of the account with organizations such as banks, credit card companies, online retailers, etc. is a very large part of what gives them assurance that my claimed identity is legitimate. Past revisions of SP 800-63 have recognized that continual use of the identity/credentials resulting in uncontested transactions is as good an indicator of the person's legitimacy as proofing new pieces of third-party evidence: NIST SP 800-63-2, pg 38 -- At Level 3, such institutions may issue credentials to their customers via the mechanisms normally used for online banking or brokerage credentials and may use online banking or brokerage credentials and tokens as Level 3 eauthentication credentials and tokens, provided: 1. The customers have been in good standing with the institution for a period of at least 1 year prior to the issuance of e-authentication credentials,	Create a set of circumstances for allowing identity assurance level (IAL) to increase as a result of regular activity directly with the person over time. Change bullet 4 to "...based on account *inactivity*..."
	63A	Preface	-	14	Ryan Galluzzo's name is repeated	Remove line #14
	63A	Preface	-	27	Ryan Galluzzo's name is repeated	Remove line #27
	63A	Preface	-	99	Ryan Galluzzo's name is repeated	Remove line #99

	63A	2.1.1	7	540	"The CSP employs one of the IAL2 Verifcation Pathways to confirm" refers to one of the pathways - How about referencing that pathway in the document to add clarity?	The CSP employs one of the IAL2 Verifcation Pathways, as described in Section 4.2.6 to confirm…
	63A	2.1.3	8	597	Regarding the "video session with a proofing agent" reference, it may be of value to clarify if this also includes Trusted Referee.	video session with a proofing agent or trusted referee
	63A	2.2	9	627	When providing example of "unique identifiers in government records (e.g., SSN, TIN, Driver's License #)", it could be useful to include passport # also as an example since many may not have the other listed documents.	in government records (e.g., SSN, TIN, Driver's License #, Passport #)
	63A	3.1.2.1	18	914, 915	If one is going to"evaluate the length of time a phone or other account has existed without substantial modifications or changes" it would be beneficial to also evaluate email domains in the same way.	Evaluate the length of time a phone, email domain or other account has existed without substantial modifications or changes.
	63A	3.1.2.1	18	919	When evaluating transaction characteristics, "such as IP Addresses, geolocations, and transaction velocities" it would be beneficial to include fraudulent, temporary, and disposable email domains to the list of characteristics to evaluate.	such as IP Addresses, geolocations, fraudulent, temporary, disposable email domains, and transaction velocities
	63A	6	53	1991	Note that each of the threats in Section 6, Threats and Security Considerations, fall under the broad category of fraud: Impersonation, False or Fraudulent Representation, Infrastructure (this last one is a target for attempting one of the first two (not a threat in itself) and is rightfully deemed out of scope immediately thereafter). From that standpoint, convergence of Digital Identity and Fraud programs lead to greater efficiency and effectiveness. This document could be more effective in its role protecting agencies if it framed the identity assurance levels as a set of controls for preventing identity-related fraud. Instead, the document leaves the impression that its function is to provide an instruction manual for the trusted external CSP market.	Allow for a greater number of approaches in the IAL process for agencies to use to protect themselves and be compliant with NIST SP 800-63.
	63B	1	1	377	"The authentication of claimants is central to the process of associating a subscriber with their online activity as recorded in their subscriber account, which is maintained by a credential service provider (CSP)." It is unclear what "which is maintained by the CSP" is referring to. Because the phrase "as recorded by their subscriber account" is subordinate to "their online activity" this sentence seems to say the CSP maintains associations between the subscriber and their "online activity" (i.e., within the RPs). I believe that NIST would like to make it clear the CSPs are not to track online activity within the RPs.	"The authentication of claimants is central to the process of associating a subscriber's ~~with their~~ online activity ~~as recorded in their subscriber account, which is~~ with the identity maintained by a credential service provider (CSP)."
	63B	1	2	412	"Applications assessed at AAL2 must offer a phishing-resistant authentication option." This requirement may significantly reduce adoption/compliance at AAL2 within agencies because it results in increased complexity and cost. - Complexity. Many CSPs support only one method of authentication as it meets their current needs. - Cost. Hardware cryptographic authenticators are significantly more expensive to issue, maintain, and recover	The requirement for phishing resistance will limit adoption significantly. Thus we suggest changing to "must" to "SHOULD offer a phishing-resistent authentication option."
	63B	2.2.2	7	582	"Verifiers SHALL offer at least one phishing-resistant authentication option at AAL2, as described in Sec. 3.2.5." This requirement may significantly reduce adoption/compliance at AAL2 within agencies because it results in increased complexity and cost. - Complexity. Many CSPs support only one method of authentication as it meets their current needs. - Cost. Hardware cryptographic authenticators are significantly more expensive to issue, maintain, and recover	The requirement for phishing resistance will limit adoption significantly. Thus we suggest changing to "must" to "SHOULD offer a phishing-resistent authentication option."
	63B	3.1.1.2	14	743	"When processing a request to establish or change a password, verifiers SHALL compare the prospective secret against a blocklist that contains known commonly used, expected, or compromised passwords. The entire password SHALL be subject to comparison, not substrings or words that might be contained therein. " The second sentence seems like an requirement that could cause security issues and should be up to the CSP. There are a number of substrings that I may wish to prevent, including: Not using "password" in your password, prohibitting two commonly used passwords concatonated together, parts of the persons name, etc... As NIST SP 800-63 revs 0-2 pointed out, an attacker can try an insecure password against every user until the attacker finds an account that used it (rather than try every password against a single account). This revision seems to rely heavily on throttling password attempts against individual users' accounts. To better protect all users, the CSP needs to ensure the password is strong as well as the throttling mechanism. Both are required.	Recommend allowing interrogation of substrings. Suggested language: "The entire password ~~SHALL~~ SHOULD be subject to comparison, ~~not~~ including substrings or words that might be contained therein. "

	63C	3.2.3	12	Fig 1.	While a proxy federation is very useful in simplifying technical integrations between traditional IdP and RPs, NIST's suggestion of suggesting a Wallet in Fig 1. Proxy Federation does not align with the wallet's defintion of a subscriber controlled artifact. The market offerings of digital wallets for citizens (barring payment wallets) are strictly subscriber controlled, and present directly to a verifier.	Consider qualifying the diagram description to state that wallet is not typical in the Proxy layer of a Proxy Federation
	63C	5.3	71	2539	Regarding: "The trust agreement for a transaction involving a subscriber-controlled wallet SHALL be established between the RP and the CSP." Often, the intention of the wallet is to store identity evidence that can be used to determine trust in the person without the involvement of an external CSP. Like a traditional wallet, the digital wallet holds photo IDs, membership cards, transaction receipts, etc. This sentence is unclear as to whether digital wallets, or the contents therein, are parties in a trust relationship. The identity evidence in SP 800-63A is not subject to prearranged trust relationships, so it is unclear why digital evidence would be. Furthermore, RPs may leverage digital wallets wholy outside of their interaction with the CSP to verify a particular attribute (e.g., bank account). Care should be taken to avoid inaccurately categorizing and therefore compressing this industry-driven paradigm into the "CSP market" model.	We suggest making it very clear that trustworthiness of the digital wallets and their contents is determined by the CSP and/or RP leveraging them. No trust agreement with the wallet or its content issuers are required in order for them to be used.
	63C	5.3	71	2545	The way this sentence is written is confusing and the meaning of the sentence is unclear: "Even though the wallet is not usually involved in the process of establishing the trust agreement, the trust agreement between the RP and CSP can still be accomplished in either an a priori or subscriber-driven fashion." The sentence seems to be taking about the role of the wallet in the trust agreement between RP and CS. These are all relvant questions that could be asked to better clarify the current language: - Do you mean to say that CSPs should convey which wallets/content issuers it leverage to the RP? - What subscriber-driven methods or determining trust with a CSP are acceptable? - What priori knowledge is needed to satisfy trust (SP 800-63A evidence requirements)?	Please consider expanding upon the meaning of the sentence with additional context and consider including an example for better understanding of the readers.
	63C	5.3	70	Fig 13	The authentication flows reference "Request federated authentication" as a federated transaction. In most cases the RP may not have a trust relationship with the wallet, such as one that a RP would have a traditional IdP. This may be confusing to some readers of the guidance.	Please consider separating traditional federation flows from wallet flows to allow for a more clear and direct understanding of the subscribe controlled wallet process. This is because trust between RP and Wallet is convyed via the CSP (issuer), and is not pre established between RP and a wallet acting as IdP.